UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/697,756	10/30/2003	Man-Pyo Hong	587-33	8762

7590 01/11/2008

ROCCO S. BARRESE, ESQ.
DILWORTH & BARRESE, LLP
333 Earle Ovington Blvd.
Uniondale, NY 11553

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
01/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/697,756	HONG ET AL.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3 remain for examination. The correspondence filed 10/15/07 amended claim 1.

Response to Arguments

2. Applicant's arguments with respect to claims 1-3 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Intrusion Detection Using Static Analysis" (hereinafter, "Wagner") in view of "Static Analysis" (hereinafter, "Webb") and further in view of Ko et al (U.S. Patent 6,697,950).

Regarding claim 1:

Wagner discloses a method for detecting malicious scripts using a static analysis, comprising the step of: checking whether a series of methods constructing a malicious code pattern exist (page 158, 1st paragraph); wherein the checking step comprises the steps of: classifying, by modeling a malicious behavior in such a manner that it includes a combination of unit behaviors each of which is composed of sub-unit behaviors or one or more method calls, each unit behavior and method call sentence

into a matching rule for defining sentence types to be detected in script codes and a relation rule for defining a relation between patterns matched so that the malicious behavior can be searched by rule variables used in the sentences satisfying the matching rule (section 4.3, "The abstract stack model", and particularly pages 160-161, "The context-free model"); generating instances of the matching rule by searching for code patterns matched with the matching rule from a relevant script code to be detected [i.e., actually implementing the classification step above] (Ibid, and also page 164, "6. Evaluation", 1st paragraph); and generating instances of the relation rule by searching for instances satisfying the relation rule from a set of the generated instances of the matching rule (Ibid).

Wagner does not disclose extracting parameters of functions used in the searched code patterns, and storing the extracted parameters in the rule variables, preferring instead to implement a simpler model. Nevertheless, Webb teaches that the ability to statically analyze "local variables, data structures, and all other data flow" in a script so as to determine if the script is non-hazardous has been long since known in the art, and has even been realized in pre-existing products (the MALPAS system, see page 4/2, and in particular the "Control Flow Analyzer", "Data Use Analyzer", and "Information Flow Analyzer" sections). It would have been quite obvious to one of ordinary skill in the art at the time the invention was made to incorporate at least these elements of Webb's MALPAS system into the static analyzer disclosed by Wagner. One might be inclined to do so because it would negate the need to make simplistic assumptions regarding the behavior of the scripts to be tested (see Wagner, page 158,

"4. Models", 2nd paragraph, noting that the conditions assumed to be true can actually be tested by Webb's "Data Use Analyzer"), and that a suitably modified analyzer would be useful to verify the correctness of many diverse and/or high integrity applications (Webb, page 4/3, "5. Static Analysis Experience and Applicability").

Neither reference explicitly discloses checking whether parameters and return values associated with the methods match each other. However, Ko discloses an analogous static analyzer employing this limitation (col. 6, lines 1-50). The claim is thus rendered obvious because all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Regarding claim 2:

Wagner further discloses wherein the matching rule is composed of rule identifiers and sentence patterns constructing malicious behavior and having the same grammar as a language of the scripts to be detected (Figure 2), and wherein the relation rule comprises conditional expressions in which conditions satisfying the relevant rule are described, and action expressions in which contents to be executed are described when the conditions in the conditional expressions are satisfied (Figure 2).

Regarding claim 3:

Wagner further discloses wherein the relation rule includes preconditions that should be satisfied prior to the conditions in the conditional expressions are described (page 162, "Principle 1" and subsequent paragraphs), and the action expressions describe contents that will be executed when both the conditional expressions and preconditions are satisfied (Fig. 2).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
12/14/07

THANHNGA TRUONG
PRIMARY EXAMINER